Claims

1. A portable data storage device comprising:

a non-volatile memory for storing user data,

an interface section for receiving data from and transmitting data to a host,

a master control unit for transferring data to and from the non-volatile memory, and

integrated circuit means for generating at least one key,

the device being arranged, upon receiving a command from a host requesting data, to transmit the requested data stored in its memory to the host using the interface section, and to transmit a key generated by the integrated circuit means to the host using the interface section.

2. A device according to claim 1 in which the generated key is transmitted in a form encrypted using a secret key which is permanently stored in the portable storage device, the portable storage device further being arranged to verify a digital signature generated by the host using the generated key and the requested data.

3. A device according to claim 2 in which the digital signature is produced by hashing the received data to generate a hash result, and encrypting the hash result using the generated key.

4. A device according to any preceding claim in which the generated key is one key of a public key/private key pair.

5. A device according to claim 4 in which the verification of the digital signature is performed in the device using the public key.

6. A device according to claim 1 in which the integrated circuit means is arranged to generate the generated key as one of a public key and a private key, the device being further arranged to generate a digital signature using the requested data and the private key, and transmits the digital signature and the public key out of the device.

7. A device according to claim 6 in which the requested data includes both data present in the memory, and also biometric data obtained from a biometric sensor of the device.

8. A device according to any preceding claim arranged to transmit the requested data in an encrypted form.

9. A device according to any preceding claim comprising a biometric sensor and verification engine for granting access to data stored in the device based on a biometric verification of the user's identity by comparison of biometric data received using the biometric sensor with pre-stored biometric data.

10. A device according to any preceding claim including a compression algorithm for exploiting any redundancy in data received by the device to compress it before storing it in the non-volatile memory, and a decompression engine to regenerate the data before it is transmitted from the device.

11. A device according to any preceding claim in which the interface section include a USB connector and a USB interface device.

12. A device according to claim 11 in which the connector is a USB plug integral with the memory device.

13. A device according to claim 12 in which the interface section is for wireless communication with a host.

14. A device according to any preceding claim having a housing, the including a narrowed end for use as a pointer.

15. A device according to any preceding claim further including a camera for generating image data, and/or a microphone for capturing audio data, the master control unit being arranged to store the image data and/or audio data in the memory.

16. In combination, a portable data storage device according to any preceding claim and a host computer, the host computer being arranged to transmit a command to the device using the interface section to request data.

17. A combination according to claim 16 wherein the device is according to claim 2, the host being arranged to generate a digital signature using the private key and the requested data.

18. A combination according to claim 16 wherein the device is according to claim 6, the host being arranged to use the public key to verify that the requested data it receives is the same data which the device used to generate the digital signature.

19. A method of transferring data from a portable data storage device to a host, the method comprising:

receiving an instruction from a host requesting data stored in a non-volatile memory of the device;

generating at least one key within the device;

obtaining the requested data from the non-volatile memory within the device; and

transmitting to the host the requested data and the key.

20. A method according to claim 19 in which the generated key is transmitted in a form encrypted using a secret key which is permanently stored in the portable storage device, the portable storage device further being arranged to verify a digital signature generated by the host using the generated key and the requested data.

21. A method according to claim 20 wherein the host generates a digital signature using the private key and the requested data.

22. A method according to claim 20 or 21 in which the digital signature is produced by hashing the received data to generate a hash result, and encrypting the hash result using the generated key.

23. A method according to any of claims 19 to 22 in which the generated key is the private key of a public key/private key pair.

24. A method according to claim 23 in which the verification of the digital signature is performed in the device using the public key.

25. A method according to claim 19 in which the generated key is generated as one of a public key and a private key, the method further comprising the device generating a digital signature using the requested data and the private key, and transmitting the digital signature and the public key out of the device.

26. A method according to claim 25, further including the host using the public key to verify that the requested data it receives is the same data which the device used to generate the digital signature.

27. A method according to claim 25 or 26 in which the requested data includes both data present in the memory, and also biometric data obtained from a biometric sensor of the device.

28. A method according to any of claims 19 to 27 in which the requested data is transmitted from the device to the host in an encrypted form.

29. A method according to any of claims 19 to 28 further comprising verifying the user's identity by comparison of biometric data received using the biometric sensor with pre-stored biometric data, and upon this verification for granting access to data stored in the device.

30. A method according to any of claims 19 to 29 including:

the device receiving data from the host, the device exploiting any redundancy in data to compress it, and the device storing it in the non-volatile memory; and

upon the data being requested by the host regenerating the data and transmitting it from the device.